



Version 14

Integration von NoSpamProxy

- in Office 365
- in Microsoft Azure
- als On-Premises-Lösung

Rechtliche Hinweise

Alle Rechte vorbehalten. Dieses Dokument und die darin beschriebenen Programme sind urheberrechtlich geschützte Erzeugnisse der Net at Work GmbH, Paderborn, Bundesrepublik Deutschland. Änderungen vorbehalten. Die in diesem Dokument enthaltenen Informationen begründen keine Gewährleistungs- und Haftungsübernahme seitens der Net at Work GmbH. Die teilweise oder vollständige Vervielfältigung ist nur mit schriftlicher Genehmigung der Net at Work GmbH zulässig.

Copyright © 2023 Net at Work GmbH

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn
Deutschland

Microsoft®, Windows®, Microsoft Exchange®, SQL Server®, SQL Server Express®, Windows Server 2008®, Windows Server 2012®, Windows Server 2012 R2®, Windows Server 2016®, Microsoft .NET Framework®, Microsoft Report Viewer®, Microsoft Office®, Microsoft 365®, Office 365®, Microsoft Outlook®, Microsoft Visual Studio® und Azure® sind eingetragene Handelsmarken der Microsoft Corporation. NoSpamProxy® und 32Guards® sind eingetragene Handelsmarken der Net at Work GmbH. Alle anderen verwendeten Handelsmarken gehören den jeweiligen Herstellern beziehungsweise Inhabern.

DIESES DOKUMENT WURDE ZULETZT AM 27. NOVEMBER 2023 ÜBERARBEITET.

Inhalt

Einleitung	1
Microsoft 365 als Relayhost freigeben	2
Weiterleitung an Microsoft 365 einrichten	5
Microsoft 365 konfigurieren	9
Die Transportregel erstellen	13
Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online	15
Schritt 1: Anlegen eines eingehenden Connectors für die Domain *	15
Schritt 2: Anlegen einer Transportregel zur Abschaltung des Spamfilters	21
Notwendige Konfigurationen für den Betrieb in Microsoft Azure	24
Hilfe und Unterstützung	30

Einleitung

Seit Version 10 ist NoSpamProxy® vollständig in Microsoft 365 integrierbar. Dieses Handbuch beschreibt die Konfigurationsschritte sowohl für NoSpamProxy und Microsoft 365 als auch für die eingesetzte Serverumgebung.

Die beschriebene Konfiguration gilt dabei ebenso für den Einsatz von NoSpamProxy als On-Premises-Lösung und in Microsoft Azure.



HINWEIS: Die spezifischen Konfigurationsschritte für den Einsatz in Microsoft Azure werden unter **Notwendige Konfigurationen für den Betrieb in Microsoft Azure** beschrieben.

Microsoft 365 als Relayhost freigeben

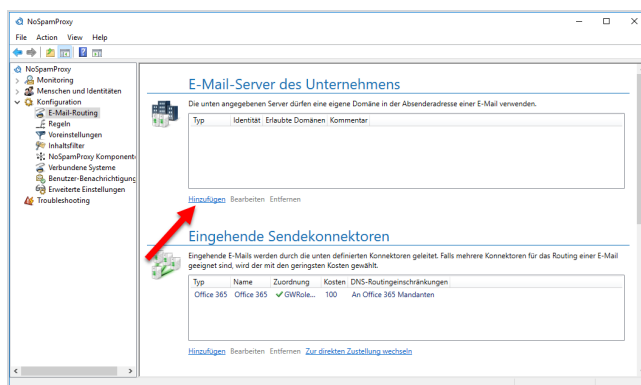
In diesem Schritt lassen Sie Microsoft 365 in der NoSpamProxy®-Konfiguration als Relayhost zu, damit E-Mails aus Microsoft 365 heraus durch NoSpamProxy an externe Kommunikationspartner verschickt werden können.

Ohne diese Konfiguration wird NoSpamProxy E-Mails als Relay-Missbrauchsversuch bewerten und abweisen.



HINWEIS: Stellen Sie sicher, dass Sie mindestens eine Unternehmensdomäne eingerichtet haben, bevor Sie mit der Konfiguration beginnen.

1. Wechseln Sie im NoSpamProxy Command Center zu **Konfiguration > E-Mail-Routing** und klicken Sie **Hinzufügen**.



2. Wählen Sie den Typ **Als Office 365 Mandant** und klicken Sie danach **Weiter**.

The screenshot shows a window titled 'E-Mail-Server des Unternehmens verwalten'. The main heading is 'E-Mail-Server des Unternehmens verwalten'. Under the heading 'Typ', there is a sub-heading 'Wählen Sie die Art wie sich der Server identifiziert.' followed by four radio button options: 'Mit einer IP-Adresse, einem Subnetz oder einem DNS-Hostnamen', 'Mit einem TLS-Client-Zertifikat', 'Als Office 365 Mandant' (which is selected and has a red arrow pointing to it), and 'Mit einer bestimmten Absenderadresse'. At the bottom of the window are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

3. Treffen Sie unter **Zugangspunkt** die für Ihre Organisationsumgebung passende Auswahl.
4. Geben Sie ihre Mandanten-ID ein. Achten Sie darauf, dass Sie den Namen der ID eingeben (nicht die ID in hexadezimaler Schreibweise).
5. Klicken Sie **Weiter**.

The screenshot shows the same window as the previous one, but now at the 'Office 365 Mandant' step. The sub-heading is 'Office 365 Mandant' and the text below it says 'Office 365 Server, die die unten angegebene Mandanten-ID angeben, werden als E-Mail-Server des Unternehmens eingestuft.' There is a dropdown menu for 'Zugangspunkt' with 'Standard Azure Cloud' selected. Below that is a text input field for 'Mandanten-ID' containing 'nsptest' and a '.onmicrosoft.com' suffix. At the bottom are the same three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

6. Wählen Sie unter **Zugeordnete Unternehmensdomänen** die Domänen aus, die Sie in Microsoft 365 hinterlegt haben und die in der Absenderadresse für ausgehende E-Mails vorkommen werden.



HINWEIS: Wenn Sie hier nicht alle Domänen vorfinden, müssen Sie die fehlenden Domänen unter **Identitäten > Unternehmensdomänen > Unternehmensdomänen** hinzufügen. Dies ist auch zu einem späteren Zeitpunkt möglich.

7. Klicken Sie **Weiter**.
8. Geben Sie bei Bedarf einen Kommentar ein und klicken Sie dann **Fertigstellen**.

Der E-Mail-Server ist nun angelegt.

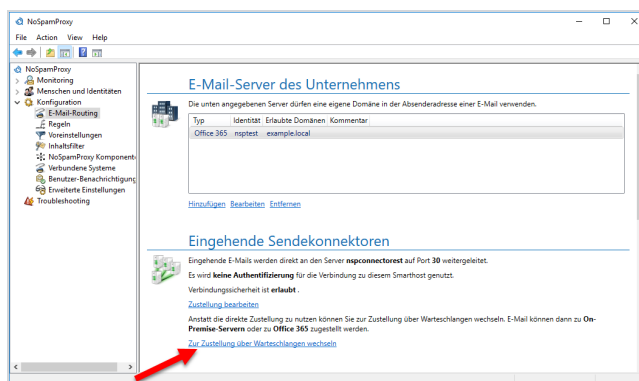
Weiterleitung an Microsoft 365 einrichten



HINWEIS: Für die Einrichtung der Weiterleitung an Microsoft 365 ist ein TLS-Zertifikat erforderlich, dass von einer von Microsoft vertrauten Stammzertifizierungsstelle ausgestellt wurde. Eine aktuelle Liste der vertrauten Stellen finden Sie unter <https://docs.microsoft.com/en-us/security/trusted-root/participants-list>.

In diesem Schritt konfigurieren Sie NoSpamProxy® so, dass alle eingehenden E-Mails an Microsoft 365 weitergeleitet werden. Dazu müssen Sie die entsprechenden Sendekonnektoren bearbeiten.

1. Wechseln Sie zu **Konfiguration > E-Mail-Routing**.
2. Klicken Sie unter **Eingehende Sendekonnektoren** auf **Zur Zustellung über Warteschlangen wechseln**.

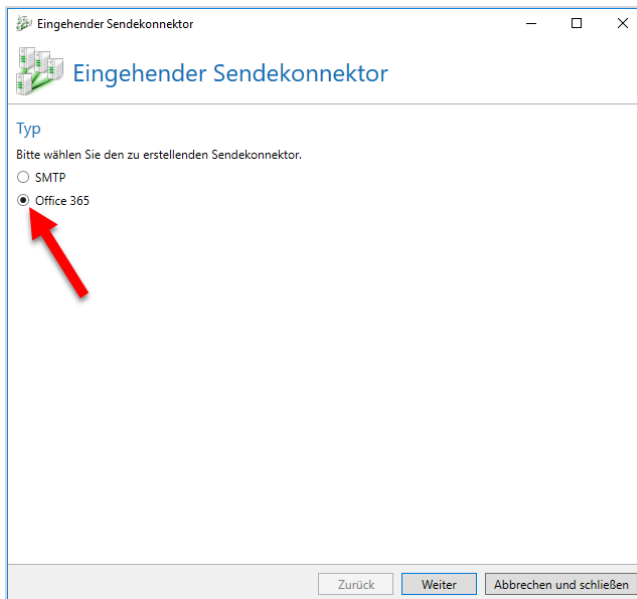


3. Wählen Sie im Dialog **Zustellung ändern** die Option **Zustellung ersetzen**.



HINWEIS: Ab Version 13 entfällt dieser Schritt, da die direkte Zustellung ab dieser Version nicht mehr unterstützt wird.

4. Wählen Sie im dann folgenden Dialog **Office 365** und klicken Sie **Weiter**.



5. Geben Sie einen beliebigen Namen für den eingehenden Sendekonnektor ein und wählen Sie danach die Gatewayrolle(n) aus, die E-Mails an Office 365 verarbeiten sollen.

6. Klicken Sie **Weiter**.

The screenshot shows the 'Eingehender Sendekonnektor' configuration window. The title bar reads 'Eingehender Sendekonnektor'. The main heading is 'Eingehender Sendekonnektor'. Under the sub-heading 'Allgemeine Einstellungen', there is a text input field for 'Name' containing 'Office365'. Below it, a note says 'Ordnen Sie diesen Konnektor allen notwendigen Gateway Rollen hinzu.' and a checkbox 'Zugeordnete Gateway Rollen' is checked. A second note states 'Wenn E-Mails identische Ziele besitzen werden die Kosten für die Auslieferung unten definiert. Der Konnektor mit den geringsten Kosten wird für den Versand gewählt.' Below this, a slider for 'Die Kosten betragen' is set to '100'. At the bottom, there are three buttons: 'Zurück', 'Weiter', and 'Abbrechen und schließen'.

7. Klicken Sie **Zertifikat auswählen**, um ein Zertifikat für die Client-Identität anzugeben, mit dem sich NoSpamProxy beim Office-365-Server authentifizieren kann.

The screenshot shows the 'Eingehender Sendekonnektor' configuration window, now on the 'Client-Identität' tab. The title bar reads 'Eingehender Sendekonnektor'. The main heading is 'Eingehender Sendekonnektor'. Under the sub-heading 'Client-Identität', a note says 'Dieses Zertifikat wird genutzt um die Client-Identität sicher zu stellen.' Below this, the sub-heading 'Client-Identität' is followed by the text 'Kein Zertifikat ausgewählt.' and 'Falls sich Ihr Zertifikat auf einer Smartcard befindet, benötigen Sie im Allgemeinen eine PIN, um darauf zuzugreifen.' There is a text input field for 'Zertifikats-PIN' with a visibility icon. Below the field are two buttons: 'Zertifikat auswählen' and 'Zertifikat entfernen'. A red arrow points to the 'Zertifikat auswählen' button. At the bottom, there are three buttons: 'Zurück', 'Fertigstellen', and 'Abbrechen und schließen'.

8. Wählen Sie im dann folgenden Dialog das TLS-Zertifikat aus, das Sie zuvor bei einer von Microsoft vertrauten Stammzertifizierungsstelle beantragt haben und klicken Sie danach **Auswählen und schließen**.
9. Klicken Sie **Auswählen und schließen**.
10. Klicken Sie im folgenden Dialogfenster **Fertigstellen**.
11. Öffnen Sie unter **Empfangskonnektoren** den genutzten Empfangskonnektor und wechseln Sie zur Registerkarte **Verbindungssicherheit**.
12. Wählen Sie entweder das von NoSpamProxy mitgelieferte oder das zuvor beantragte Zertifikat aus.
13. Klicken Sie **Auswählen und schließen** und dann **Speichern und schließen**.

Die Konfiguration für NoSpamProxy ist nun abgeschlossen.

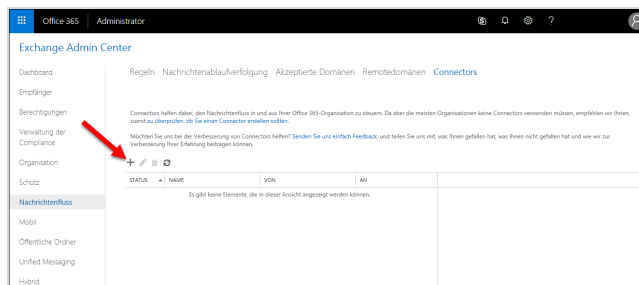
Microsoft 365 konfigurieren

In diesem Schritt konfigurieren Sie den Office-365-Mandanten so, dass ausgehende E-Mails nicht direkt an den Empfängerserver, sondern zunächst an NoSpamProxy® zugestellt werden. Melden Sie sich dazu in an Ihrem Office-365-Mandanten unter <https://outlook.office365.com/ecp> an.



HINWEIS: Verwenden Sie für die Anmeldung einen Benutzer, der über Administrationsrechte verfügt.

1. Wechseln Sie im Exchange Admin Center zu **Nachrichtenfluss > Connectors**; klicken Sie danach das **Plus-Zeichen**. Der Assistent zum Anlegen eines neuen Connectors öffnet sich.



2. Wählen Sie auf der ersten Seite im Feld **Von** die Option **Office 365** aus; wählen Sie im Feld **An** die Option **Partnerorganisation** aus.
3. Klicken Sie **Weiter**. Mit dieser Einstellung werden ausgehende E-Mails vom Office-365-Mandanten an NoSpamProxy gesendet.
4. Geben Sie auf der dann folgenden Seite einen beliebigen Namen für den Connector ein.
5. Geben Sie bei Bedarf eine Beschreibung ein und klicken Sie **Weiter**.

6. Wählen Sie auf der dann folgenden Seite die Option **Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Konnektor umleitet**.

7. Klicken Sie **Weiter**.

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

Neuer Connector

Wann möchten Sie diesen Connector verwenden?

Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an diesen Connector umleitet

Nur, wenn ich eine Transportregel eingerichtet habe, die Nachrichten an alle akzeptierten Domänen in Ihrer Organisation gesendete E-Mails umleitet

Nur, wenn E-Mails an diese Domänen gesendet werden

+ -

Zurück Weiter Abbrechen

8. Geben Sie den Namen oder die IP-Adresse des Servers (Smarthost) an, auf dem die Gatewayrolle installiert ist und klicken Sie danach **Speichern**.

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

smarthost hinzufügen

Geben Sie den vollqualifizierten Domännennamen (FQDN) des Smarthosts oder eine IPv4-Adresse an.
Beispiel: „myhost.contoso.com“ oder „192.168.3.2“

nsp-cloudonly.cloudapp.net

Speichern Abbrechen



HINWEIS: Beachten Sie beim Eintragen des Hostnamens, dass Microsoft 365 bei der Auflösung die MX-Einträge vor den A-Einträgen betrachtet. Sollte für den eingetragenen Hostnamen neben einem A-Eintrag auch ein MX-Eintrag existieren, wird der Konnektor auf diesen zurückgreifen.

9. Aktivieren Sie im folgenden Dialogfenster die Option **Immer TLS zum Sichern der Verbindung verwenden**. Im darunterliegenden Dialogfenster wählen Sie den Punkt **Alle digitalen Zertifikate, einschließlich selbstsignierter Zertifikate** aus und klicken **Weiter**.

https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

Neuer Connector

Wie sollte Office 365 eine Verbindung mit Ihrem E-Mail-Server herstellen?

Immer TLS (Transport Layer Security) zum Sichern der Verbindung verwenden (empfohlen)
Verbindung nur herstellen, wenn das Zertifikat des E-Mail-Servers des Empfängers dieses Kriterium erfüllt

Alle digitalen Zertifikate, einschließlich selbstsignierter Zertifikate

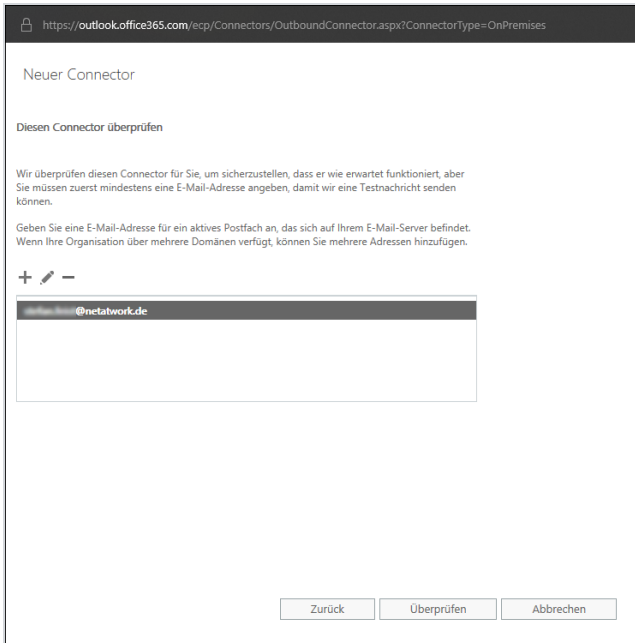
Nur von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt

Nur, wenn der Antragstellername oder der alternative Antragstellername (SAN) mit diesem Domänennamen überein:
Beispiel: "contoso.com" oder "*.contoso.com"

Zurück Weiter Abbrechen

10. Kontrollieren Sie die Zusammenfassung Ihrer Angaben auf Richtigkeit und klicken Sie **Weiter**.

11. Geben Sie im folgenden Dialog eine oder mehrere E-Mail-Adressen ein, die Sie für die Überprüfung dieses Konnektors verwenden möchten.



https://outlook.office365.com/ocp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises

Neuer Connector

Diesen Connector überprüfen

Wir überprüfen diesen Connector für Sie, um sicherzustellen, dass er wie erwartet funktioniert, aber Sie müssen zuerst mindestens eine E-Mail-Adresse angeben, damit wir eine Testnachricht senden können.

Geben Sie eine E-Mail-Adresse für ein aktives Postfach an, das sich auf Ihrem E-Mail-Server befindet. Wenn Ihre Organisation über mehrere Domänen verfügt, können Sie mehrere Adressen hinzufügen.

+ ✎ -

@nctatwork.de

Zurück Überprüfen Abbrechen

12. Klicken Sie **Überprüfen**.

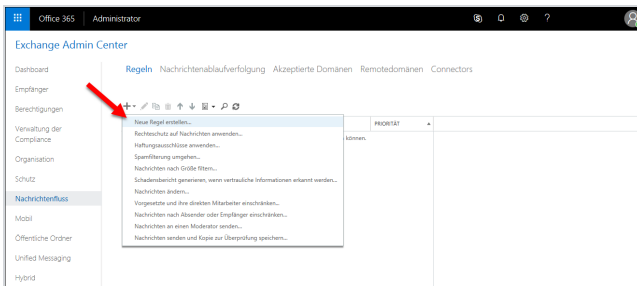


HINWEIS: Es werden nun eine oder mehrere Test-Nachrichten gesendet. Nach Abschluss der Prüfung erhalten Sie ein Überprüfungsergebnis. Die Test-Nachricht schlägt in der Regel fehl; dies können Sie zunächst ignorieren.

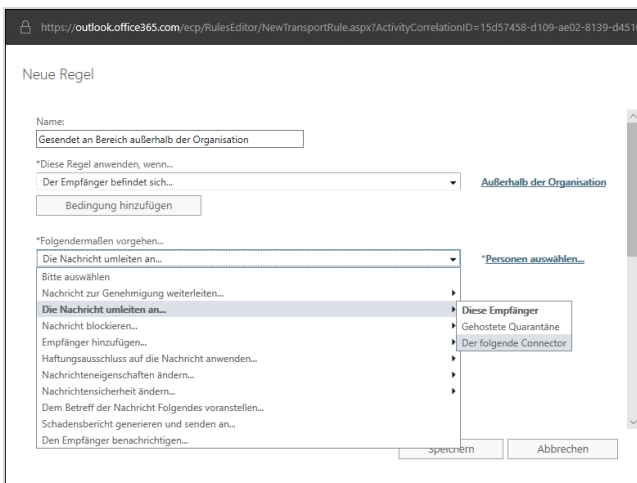
13. Klicken Sie **Speichern**, um den Dialog zu schließen.

Die Transportregel erstellen

1. Gehen Sie in der Office-365-Verwaltungsoberfläche zu **Nachrichtenfluss > Regeln**.
2. Klicken Sie das **Plus-Symbol**.



3. Wählen Sie danach die Option **Neue Regel erstellen**. Der Assistent für die Erstellung einer neuer Transportregel öffnet sich.



4. Geben Sie einen beliebigen Namen für die Regel ein.
5. Stellen Sie unter **Diese Regel anwenden wenn** die folgenden Optionen ein:
 - **Der Empfänger befindet sich** sowie
 - **Außerhalb der Organisation**.

6. Stellen Sie unter **Folgendermaßen vorgehen** die Option **Folgenden Connector verwenden** ein.
7. Geben Sie danach den vorher erstellten Konnektor an und klicken Sie **OK**.



HINWEIS: Falls Sie an dieser Stelle nur **Personen** auswählen können, klicken Sie im unteren Abschnitt **Weitere Optionen**. Dort können Sie unter **Die Nachricht umleiten an** die Option **Folgenden Connector verwenden** auswählen. Anschließend können Sie den zuvor erstellten Konnektor verwenden.

8. Klicken Sie **Speichern**.

Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online

Wenn Sie NoSpamProxy® in Microsoft 365 in Verbindung mit Exchange Online nutzen, müssen Sie in Ihrem Tenant zusätzliche Einstellungen vornehmen, die die Spamabwehr sicherstellen.

I Schritt 1: Anlegen eines eingehenden Connectors für die Domain *

Um die Zustellung von unerwünschten E-Mails aus dem Internet zu unterbinden, legen Sie einen eingehenden Connector an. Dieser Connector erlaubt für die Domain * nur E-Mails von bestimmten IP-Adressen - Ihrem eigenen E-Mail-Server oder NoSpamProxy. Hierfür wird ein entsprechender Partner Connector benötigt.

Um den Partner Connector in PowerShell anzulegen, geben Sie Folgendes ein:

```
New-InboundConnector  
  
-Name "NurE-MailsVonDiesemServerAkzeptieren<NoSpamProxy>"  
  
-ConnectorType Partner  
  
-SenderDomains *
```

```
-RestrictDomainsToCertificate $true

-TlsSenderCertificateName <DasZuvorErstellteUndAusgewählteZertifikat>

-AssociatedAcceptedDomains

<AlleDomänenDieInNoSpamProxyUnterEigeneDomänenStehenUndImOffice365TenantVerwendetWerden>
```



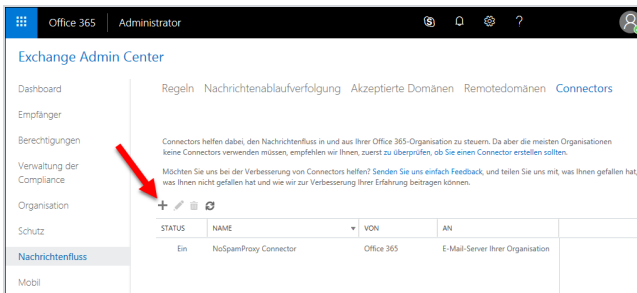
WARNUNG: Um den Spam-Schutz durch NoSpamProxy® sicherzustellen, müssen Sie sämtlichen eingehenden E-Mail-Verkehr über NoSpamProxy leiten und Microsoft 365 ausschließlich durch NoSpamProxy unter Verwendung eines dedizierten Konnektors ansprechen. Ansonsten ist es möglich, dass sich die Anti-Spam-Funktionalitäten von NoSpamProxy und Exchange Online Protection (EOP) gegenseitig behindern. Wir empfehlen Ihnen dringend, diese Einstellung vorzunehmen, da die Sicherheit und Stabilität Ihrer Konfiguration sonst nicht gewährleistet ist.



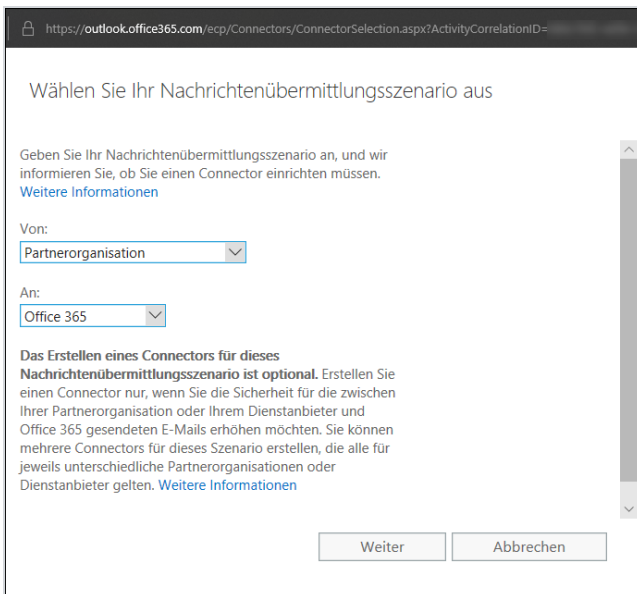
TIPP: Sie können an Stelle der IP-Adresse auch das Zertifikat des einliefernden Gateways hinterlegen.

Um den Partner Connector über das Exchange Control Panel anzulegen, gehen Sie folgendermaßen vor:

1. Gehen Sie zu **Nachrichtenfluss > Connectors** und klicken Sie das **Plus-Zeichen**.



2. Wählen Sie im Dialogfenster die Optionen **Partnerorganisation** und **Office 365** aus und klicken Sie danach **Weiter**.



3. Geben Sie im Dialog **Neuer Connector** einen Namen für den Connector ein und fügen Sie bei Bedarf eine Beschreibung hinzu. Lassen Sie das Häkchen

neben **Einschalten** gesetzt. Klicken Sie dann **Weiter**.

https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

Neuer Connector

Dieser Connector erzwingt Routing- und Sicherheitseinschränkungen für E-Mails, die von Ihrer Partnerorganisation oder Ihrem Dienstanbieter an Office 365 gesendet werden.

*Name:
Eingehender Connector via NoSpamProxy

Beschreibung:

Was möchten Sie nach dem Speichern des Connectors tun?
 Einschalten

Weiter Abbrechen

4. Wählen Sie im folgenden Dialogfenster die Option **Domäne des Absenders** und klicken Sie danach **Weiter**.

https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

Neuer Connector

Wie möchten Sie die Partnerorganisation identifizieren?

Geben Sie an, ob Sie eine Domäne oder IP-Adresse verwenden möchten, um die Partnerorganisation zu identifizieren. [Weitere Informationen](#)

Domäne des Absenders verwenden
 IP-Adresse des Absenders verwenden

Zurück Weiter Abbrechen

5. Klicken Sie im folgenden Dialogfenster das **Plus-Zeichen**.

https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

Neuer Connector

Anhand welcher Absenderdomäne möchten Sie Ihren Partner identifizieren?

Geben Sie mindestens eine Absenderdomäne an.

+ -

Zurück Weiter Abbrechen

6. Geben Sie als Domainnamen ein Sternchen ("*") ein. Klicken Sie danach **OK** und auf der folgenden Seite **Weiter**.

https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

domäne hinzufügen

Geben Sie den Domännennamen an, mit oder ohne Platzhalter.
Beispiel: * oder *.contoso.com oder *.com

*

OK Abbrechen

7. Setzen Sie auf der folgenden Seite das Häkchen bei **E-Mails zurückweisen**, wenn Sie nicht aus diesem Adressbereich gesendet werden. Klicken Sie

Weiter.

https://outlook.office365.com/ecp/Connectors/inboundPartnerConnector.aspx

Neuer Connector

Welche Sicherheitseinschränkungen sollen angewendet werden?

E-Mails zurückweisen, wenn sie nicht über TLS gesendet werden

Und anfordern, dass der Antragstellername im Zertifikat, das der Partner verwendet, um sich bei Office 365 zu authentifizieren, mit diesem Domännennamen übereinstimmt

Beispiel: "contoso.com" oder "*.contoso.com"

E-Mails zurückweisen, wenn sie nicht aus diesem IP-Adressbereich gesendet werden

+ ✎ -

Zurück Weiter Abbrechen

8. Geben Sie im Dialog **IP-Adresse hinzufügen** die Adresse des Servers an, auf dem die Gatewayrolle installiert ist. Klicken Sie **OK**.

https://outlook.office365.com/ecp/Connectors/inboundPartnerConnector.aspx

ip-adresse hinzufügen

Geben Sie eine einzelne IP-Adresse oder mehrere IP-Adressen in CIDR-Notation an.
Beispiel: 10.5.3.2 oder 10.3.1.5/24

10.5.3.2

OK Abbrechen

- Überprüfen Sie die Angaben in der Zusammenfassung auf Richtigkeit und klicken Sie **OK**.

https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx

Neuer Connector

Ihre Einstellungen bestätigen
Stellen Sie vor dem Speichern sicher, dass dies die Einstellungen sind, die Sie konfigurieren möchten.

E-Mail-Flussszenario
Von: Partnerorganisation
An: Office 365

Name
Eingehender Connector via NoSpamProxy

Beschreibung
Keine

Status
Nach dem Speichern aktivieren

So identifizieren Sie Ihre Partnerorganisation
Identifizieren Sie die Partnerorganisation, indem Sie überprüfen, ob die Nachrichten von diesen Domänen stammen: *

Sicherheitseinschränkungen
Nachrichten ablehnen, wenn sie nicht aus diesen IP-Adressbereichen stammen:

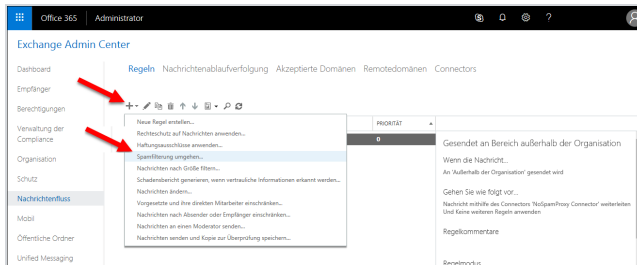
Zurück Speichern Abbrechen

Der neue Connector erscheint jetzt unter **Nachrichtenfluss/Connectors**.

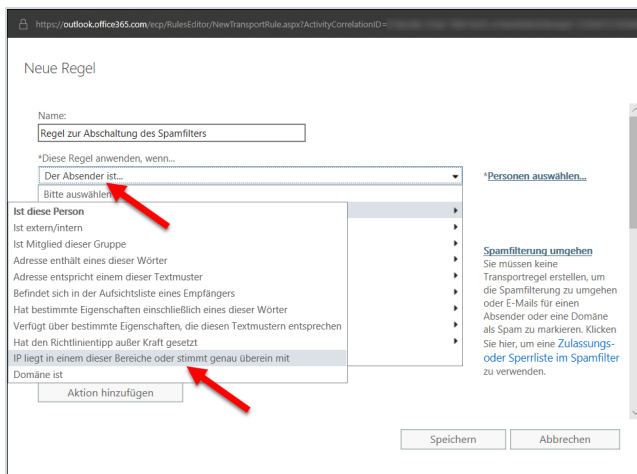
■ Schritt 2: Anlegen einer Transportregel zur Abschaltung des Spamfilters

- Gehen Sie zu **Nachrichtenfluss/Regeln**.
- Klicken Sie das **Plus-Zeichen**.
- Wählen Sie **Spamfilterung umgehen** aus dem Drop-Down-Menü.

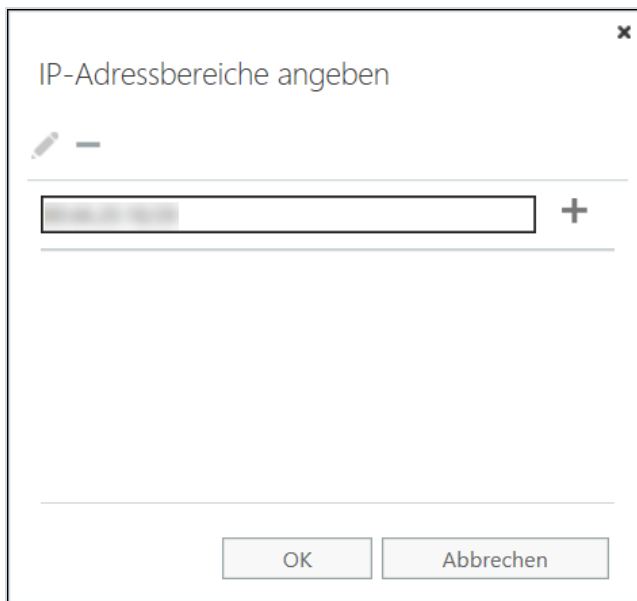
4. Geben Sie der Regel einen Namen.



5. Wählen Sie unter **Diese Regel anwenden, wenn die Option Absender und danach IP liegt in einem dieser Bereiche oder stimmt genau überein mit.**



6. Geben Sie im Dialog **IP-Adressbereiche angeben** die IP-Adresse des Servers an, auf dem die Gatewayrolle installiert ist.



7. Klicken Sie das **Plus-Zeichen** und danach **OK**.
8. Klicken Sie **Speichern**.

Die Regel ist nun eingerichtet. Der Spamschutz für die Nutzung von NoSpamProxy in Microsoft 365 mit Exchange Online ist sichergestellt.

Notwendige Konfigurationen für den Betrieb in Microsoft Azure

Einbinden des TCP Proxy



HINWEIS: Sie müssen über einen gültigen Vertrag über Softwarewartung verfügen, um den TCP Proxy nutzen zu können.

Bei einigen cloudbasierten Systemen – zum Beispiel in Microsoft Azure – kann es vorkommen, dass der Port 25 ausgehend vom Anbieter blockiert wird. Port 25 wird aber zum Versand von E-Mails benötigt, was einen Betrieb von NoSpamProxy auf einem solchen System behindert.

Hierzu bieten wir eine Alternative an, um solche Systeme trotzdem zu nutzen: unseren *TCP Proxy*. Dieses System kann auf unten beschriebene Weise in NoSpamProxy aktiviert werden. Dabei wird jede ausgehende Verbindung an eine routing-fähige IPv4-Adresse auf TCP-Ebene durch den TCP Proxy für NoSpamProxy geroutet. Die E-Mails werden dann vom Server aus über Port 443 an den TCP Proxy gesendet und von dort dann über Port 25 weiter zum Empfängersystem geleitet.

1. Stoppen Sie den Dienst der Gatewayrolle über das NoSpamProxy Command Center oder die Windows-Dienste
2. Öffnen Sie als Administrator einen Texteditor auf dem System, auf dem die Gatewayrolle installiert ist.
3. Öffnen Sie die Konfigurationsdatei **Gateway Role.config** aus dem Verzeichnis **C:\ProgramData\Net at Work Mail Gateway\Configuration**.

- Suchen Sie in der Datei nach `<smtpServicePointConfiguration>` und ändern/fügen Sie den Wert

```
isProxyTunnelEnabled="true"  
proxyTunnelAddress="proxy.nospamproxy.com"
```

als Attribute hinzu. Falls `<smtpServicePointConfiguration` nicht vorhanden ist, suchen Sie nach `<netatwork.nospamproxy.proxyconfiguration` und fügen Sie

```
<smtpServicePointConfiguration  
isProxyTunnelEnabled="true"  
proxyTunnelAddress="proxy.nospamproxy.com" />
```

direkt unter diesem Wert hinzu.

- Speichern Sie die Datei ab und schließen Sie den Editor.
- Legen Sie das **Root CA Zertifikat** im Zertifikatsspeicher von Microsoft im Computerkonto unter **Vertrauenswürdige Stammzertifizierungsstellen > Zertifikate** auf dem Server mit der Gatewayrolle ab.
- Bearbeiten Sie im NoSpamProxy Command Center unter **Konfiguration > NoSpamProxy Komponenten > Gatewayrollen** die entsprechende Gatewayrolle und ändern Sie den Wert für **SMTP Servername** auf den Wert `outboundproxy.nospamproxy.com`.
- Starten Sie den Gatewayrollen-Dienst wieder

- Öffnen Sie die Datei **Gateway Role.config** erneut und prüfen Sie, ob der Wert beim Start erhalten geblieben ist.

I Anpassen des SPF-Eintrags

- Wenn der TCP-Proxy implementiert ist, tritt dieser als absendendes System auf. Somit muss der TCP-Proxy auch mit in Ihrem SPF-Eintrag aufgenommen werden. Wir empfehlen dringend, folgenden Eintrag in Ihren SPF-Eintrag hinzuzufügen:

```
include:_spf.proxy.nospamproxy.com
```

I Gegebenenfalls: Anpassen von Microsoft 365

Falls Sie aus Azure heraus E-Mails an eine eigene Microsoft-365-Instanz schicken, bei der ein Konnektor auf die IP-Adressen gebunden ist, aktualisieren Sie bitte die IP-Adressen passend zum Namen `outboundproxy.nospamproxy.com`. Da bei Microsoft 365 die TLS-Zertifikate gegen die HELO-Domain geprüft werden, ist es nur mit deutlich erhöhtem Aufwand möglich, dies entsprechend umzusetzen. Wir empfehlen daher eine Validierung anhand des Namens.

I Gegebenenfalls: Anpassen der Firewall

- Falls Sie ausgehende Verbindungen gezielt blockieren, sollten Sie die Ausnahme für den TCP Proxy so anpassen, dass Verbindungen zum **IP-Netz 193.37.132.0/24** erlaubt sind.

Einrichten einer statischen IP-Adresse

Wenn Sie NoSpamProxy oder Teile davon in einer virtuellen Maschine in einer Microsoft-Azure-Umgebung betreiben möchten, benötigen Sie eine IP-Adresse, die auch nach dem Neustart der Maschine erhalten bleibt. Um dies zu erreichen, müssen Sie eine statische IP-Adresse (Reserved IP Address) einrichten. Ansonsten ist es möglich, dass nach dem Neustart der Maschine eine andere IP-Adresse zugewiesen wird.



HINWEIS: Diese Einstellung nehmen Sie auf dem virtuellen Computer in Microsoft Azure vor, auf dem NoSpamProxy installiert ist.

1. Öffnen Sie die Webseite portal.azure.com.
2. Klicken Sie unter **Home > Virtuelle Computer** auf den virtuellen Computer, auf dem NoSpamProxy installiert ist.
3. Gehen Sie zu **Netzwerk > Netzwerkschnittstelle > IP-Konfigurationen** und wählen Sie die für NoSpamProxy relevante Konfiguration.
4. Aktivieren Sie die Option **Öffentliche IP-Adresse** und klicken sie danach **Neu erstellen**.
5. Geben Sie einen Namen ein und wählen Sie die Option **Statisch** aus.
6. Klicken Sie **OK**.

Die IP-Adresse wird nun unter dem angegebenen Namen angezeigt.



HINWEIS: Beachten Sie beim Einrichten einer statischen IP-Adresse die Informationen von der entsprechenden [Seite der Microsoft-Dokumentation](#).

■ Anpassen des Reverse-DNS-Eintrags für den NoSpamProxy-Server

1. Öffnen Sie portal.azure.com.
2. Gehen Sie zu **Dashboard > Ressourcengruppen > [DieRessourcengruppeZuDerDerVirtuelleComputerGehoert] > [IhrVirtuellerComputer] > Eigenschaften**.
3. Geben Sie unter **DNS-Namensbezeichnung** einen Namen für die öffentliche IP-Adresse an.
4. Starten Sie die Azure Shell.
5. Geben Sie den folgenden Befehl ein und ersetzen Sie dabei die vorhandenen Platzhalter:

```
az network public-ip update --resource-group  
[Ressourcengruppe] --name [NameDerIPAdresse] --  
reverse-fqdn [VollstaendigerDNSName] --dns-name  
[DNSName]
```



HINWEIS: Beachten Sie auch die Anweisungen auf der entsprechenden [Seite der Microsoft-Azure-Dokumentation](#).

Hilfe und Unterstützung

Knowledge Base

Die **Knowledge Base** enthält weiterführende technische Informationen zu unterschiedlichen Problemstellungen.

Website

Auf der **NoSpamProxy-Website** finden Sie Handbücher, Whitepaper, Broschüren und weitere Informationen zu NoSpamProxy.

NoSpamProxy-Forum

Das **NoSpamProxy-Forum** gibt Ihnen die Gelegenheit, sich mit anderen NoSpamProxy-Anwendern auszutauschen, sich zu informieren sowie Tipps und Tricks zu erhalten und diese mit anderen zu teilen.

Blog

Das **Blog** bietet technische Unterstützung, Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und vieles mehr. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite des NoSpamProxy Command Center angezeigt.

YouTube

In unserem **YouTube-Kanal** finden Sie Tutorials, How-tos und andere Produktinformationen, die Ihnen das Arbeiten mit NoSpamProxy erleichtern.

NoSpamProxy-Support

Unser Support-Team erreichen Sie

- per Telefon unter +49 5251304-636
- per E-Mail unter support@nospamproxy.de.

